IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

In re Patent Application of:)	
DELLOW ET AL.)	
)	
Serial No. **10/817,148**)	Examiner: **D. ALMEIDA**
)	
Filing Date: **APRIL 2, 2004**)	Art Unit: **2432**
)	
For: **MEMORY SECURITY DEVICE FOR**)	Attorney Docket No.
FLEXIBLE SOFTWARE ENVIRONMENT)	**00-IMS-421/52840**
)	

APPELLANTS' APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellants' Appeal Brief together with the requisite $540.00 large entity fee for filing a brief. If any additional extension and/or fee is required, authorization is given to charge Deposit Account No. **01-0484**.

(1) Real Party in Interest

The real parties in interest are STMicroelectronics (Research & Development) Limited, Andrew Dellow of Gloucester, United Kingdom, and Peter Bennett of Bristol, United Kingdom.

(2) Related Appeals and Interferences

To Appellants' knowledge, there are no currently pending or prior related appeals, interferences, or judicial proceedings.

(3) Status of the Claims

Claims 1-19, 21-25, and 27-34 are currently pending in the present application, stand rejected, and are all being appealed herein.

Claims 20 and 26 are no longer pending in the present application, do not stand rejected, and are not appealed herein.

(4) Status of the Amendments

All amendments have been entered and there are no further pending amendments. A copy of the claims involved in this appeal is attached hereto as Appendix A.

(5) Summary of the Claimed Subject Matter

Independent Claim 1 is directed to a semiconductor integrated circuit 1 for executing application code received from a memory 2 via external connections 20. The integrated circuit
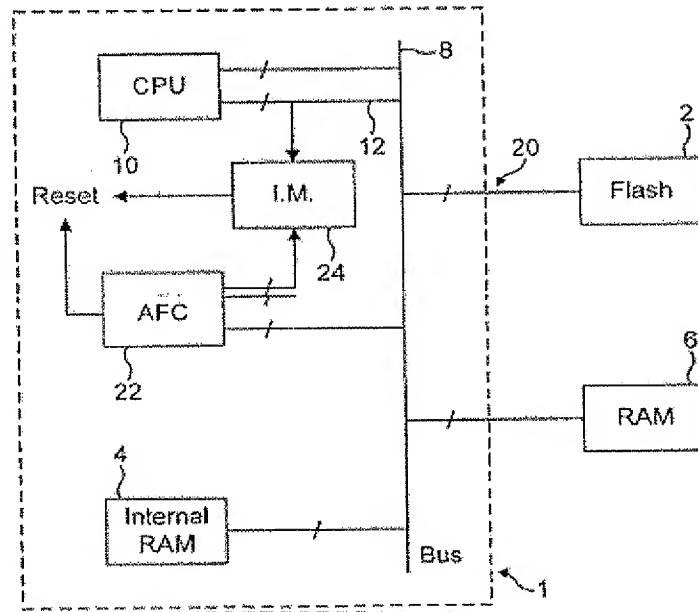
2

_____/

comprises a processor 10 to execute the application code from the
memory, an internal bus 8 to provide the application code to the
processor from the memory, and a verifier processor 22. The
verifier processor is to receive the application code via the
internal bus and continually processes the application code using
a verification function while the processor executes the
application code from the memory independently of the verifier
processor. The verifier processor is also for impairing the
function of the integrated circuit in an event that the
application code does not satisfy the verification function. The
integrated circuit further comprises an instruction monitor 24 to
monitor code requests issued by the processor and to impair the
function of the integrated circuit unless addresses of the code
requests fall within a given range. (Specification: Page 4,
lines 10-25; and Figure 1, reproduced below).

Figure 1 of the Present Application

Independent Claim 19 is directed to a semiconductor integrated circuit 1 for executing application code received from a memory 2. The semiconductor integrated circuit includes a processor 10 to execute the application code from the memory, an internal bus 8 connected to the processor to provide the application code to the processor from the memory, and a verifier processor 22. The verifier processor receives the application code via the internal bus. The verifier processor processes the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, and impairs the execution of the integrated circuit if the application code does not satisfy the verification function. The semiconductor

integrated circuit further includes an instruction monitor 24 to be connected to the internal bus, to monitor code requests issued by the processor, and to impair the execution of the integrated circuit unless addresses of the code requests fall within a given range. (Specification: Page 4, line 10 through page 6, line 27; and Figure 1, reproduced above).

Independent Claim 25 is directed to a memory system that includes a non-volatile memory 2 to store application code, and a semiconductor integrated circuit 1 to execute the application code to be received from the non-volatile memory. The integrated circuit includes a processor 10 to execute the application code from the non-volatile memory, an internal bus 8 connected to the processor to provide the application code to the processor from the non-volatile memory, and a verifier processor 22. The verifier processor receives the application code via the internal bus. The verifier processor processes the application code using a verification function while the processor executes the application code from the non-volatile memory independently of the verifier processor. The verifier processor also renders the memory system at least partly unusable if the application code does not satisfy the verification function. The integrated circuit further includes an instruction monitor 24 to be connected to the internal bus, to monitor code requests issued by the processor, and to impair the execution of the integrated circuit unless addresses of the code requests fall within a given

range. (Specification: Page 4, line 10 through page 6, line 27; and Figure 1, reproduced above).

Independent Claim 31 is directed to a method for executing application code received from an external memory 2 via external connections 20. The method includes executing application code from the external memory with a processor 10, providing the application code to the processor via an internal bus 8, and providing the application code to a verifier processor 22 via the internal bus. The method also includes continually processing the application code with the verifier processor, while the processor executes the application code independently of the verifier processor, using a verification function. The method also includes monitoring code requests issued by the processor with an instruction monitor 24, and impairing operation of the integrated circuit if the application code does not satisfy the verification function or if addresses of the code requests fall outside a given range. (Specification: Page 4, line 10 through page 6, line 27; and Figure 1, reproduced above).

(6) _Grounds of Rejection to be Reviewed On Appeal_

A. Ground One

The Examiner rejected Claims 1-4, 14-17, 19, 21-22, 24-25, 27-28, and 30-34 under 35 U.S.C. §103(a) over U.S. Patent No. 6,430,727 to Warren in view of International Publication No. WO 01/61437 to Goffin et al.

B. Ground Two

The Examiner rejected dependent Claims 10-12 under 35 U.S.C. §103(a) over the Warren patent in view of the Goffin et al. reference and further in view of U.S. Patent Application No. 2003/0229777 to Morais et al.

C. Ground Three

The Examiner rejected dependent Claims 5-9, 13, 18, 23, and 29 under 35 U.S.C. §103(a) over the Warren patent in view of the Goffin et al. reference and further in view of U.S. Patent Application No. 2003/0005277 to Harding et al.

(7) Argument

As will be described in greater detail below, Appellants respectfully request the Board of Patent Appeals and Interferences reconsider and withdraw the Examiner's rejections of the claims. As detailed herein, Appellants submit that the Examiner's proposed combination of the diagnostic tool of Warren and the secure code computing device of Goffin et al. fails to disclose the claimed invention and lacks sufficient rationale for combination.

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**

_____/

A. THE REJECTION OVER WARREN IN VIEW OF GOFFIN ET AL. IS IMPROPER

The Examiner rejected independent Claims 1, 19, 25, and 31 over Warren in view of Goffin et al. Warren discloses an integrated circuit comprising a CPU, a bus coupled to the CPU, a memory coupled to the bus, a breakpoint range unit storing first and second breakpoint addresses, and a logic controller coupled to the breakpoint range unit. The breakpoint range unit compares the instruction address currently being processed by the CPU. If the current instruction address falls within the first and second breakpoint addresses, the breakpoint range unit generates a breakpoint signal, which is received by the logic controller. Upon receipt of the breakpoint signal, the logic controller interrupts the CPU, thereby enabling diagnostic tests on the CPU. (Col. 2, lines 25-47).

The Examiner correctly notes that Warren fails to disclose "a verifier processor to receive the application code via the internal bus, wherein the verifier processor continually processes the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, and to impair the function of the integrated circuit in an event that the application code does not satisfy the verification function," as recited, for example, in independent Claim 1. The Examiner looks to Goffin et al. to supply this deficiency of Warren.

Goffin et al. discloses a first embodiment of a computing device that includes a master processor 101, a master

8

memory unit 103 coupled to the master processor via a memory bus
104, and a secure processor 102 also coupled to the memory via
the memory bus. *See* Figure 1, reproduced below. The code is
first downloaded by the master processor and stored in the master
memory unit for subsequent authentication by the secure
processor. (Page 10, line 32 through Page 12, line 12). The
secure processor receives the code via the memory bus. (Page 12,
lines 1-3). If the code is not authentic, the secure processor
can erase or disable the adulterated memory blocks or disable the
entire computing device. (Page 13, lines 12-18). The secure
processor may periodically sweep code stored in the master memory
unit for re-authentication. (Page 14, lines 5-16).
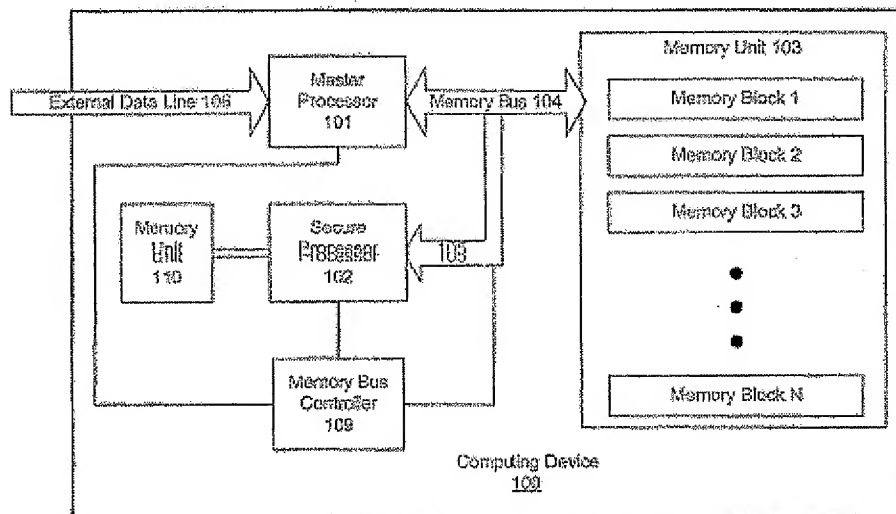
Figure 1 of Goffin et al.

In an alternative embodiment, the code is initially
received by the secure processor rather than the master

processor. (Page 12, lines 13-15). In this embodiment, the secure processor receives the code and stores it in an interim memory before long-term storage of authenticated code in the master memory unit. (Page 12, lines 13-23). Goffin et al. does not disclose how the secure processor receives the code directly. That is, in this different embodiment of Goffin et al., Goffin et al. does not disclose a verifier processor receiving the application code via the internal bus, as recited by the independent claims.

Appellants submit that Goffin et al. fails to disclose the verifier processor receiving the application code via the internal bus, and the processor executing the application code from the memory independently of the verifier processor, as recited in independent Claim 1. In the first embodiment, i.e. where the master processor first receives code and stores it for subsequent authentication, the verification routine is not independent from the master processor since it first receives the code for storage. In the second embodiment, i.e. where the secure processor receives the code first, the code is not received via the memory bus, as in the first embodiment. In other words, Goffin et al. fails to disclose both the verifier processor receiving the application code via the internal bus, and the processor executing the application code from the memory independently of the verifier processor, as recited in independent Claim 1. For this reason alone, independent Claim 1 is patentable over the prior art.

_____/

Appellants also note that Goffin et al. fails to disclose the verifier processor <u>continually</u> processing the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, as recited by independent Claim 1, for example. Differently, in Goffin et al., the authentication of the code by the secure processor is sequentially performed before any execution by the master processor. Moreover, even during re-authentication, the secure processor gives way to the master processor's use of the memory bus, for example, when the master processor is accessing code for execution. (Page 14, line 17 through Page 15, line 8). Therefore, for this additional reason, independent Claim 1 is patentable over the prior art.

The Examiner's stated motivation to combine Warren with Goffin et al. is to increase security of the system. Furthermore, Appellants submit that the Examiner's combination is improper because the prior art references teach away from such a selective combination. More particularly, Warren discloses an integrated circuit for diagnostic procedures, i.e. interrupting normal operation of the CPU to allow diagnostic procedures to be implemented. (Col. 1, lines 5-8). Differently, Goffin et al. discloses a computing device that provides for secure downloading of software. (Page 1, lines 8-25). Given that Warren deals with diagnostics and not security, Appellants submit that the person of ordinary skill in the art would be taught away from the

11

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**

Examiner's proposed selective combination. Moreover, Appellants submit that the person of ordinary skill in the art would not be motivated to combine two disparate embodiments of Goffin et al. *Cf. Boston Sci. Scimed, Inc. v. Cordis Corp.*, 2009 U.S. App. LEXIS 588 (Fed. Cir. 2009); and *GNB Battery Techs. v. Exide Corp.*, 38 U.S.P.Q.2D 1506 (Fed. Cir. 1996).

Accordingly, because of the above noted deficiencies of the prior art, independent Claim 1 is patentable over the prior art. Independent Claims 19, 25, and 31 are similar to Claim 1 and are patentable for similar reasoning. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

B. THE REJECTION OVER WARREN IN VIEW OF GOFFIN ET AL. AND MORAIS ET AL. IS IMPROPER

The Examiner rejected dependent Claims 10-12 over Warren in view of Goffin et al. and Morais et al. These dependent claims are patentable as being dependent upon patentable independent claims, such patentability established in the arguments above.

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**

C. THE REJECTION OVER WARREN IN VIEW OF GOFFIN ET AL. AND HARDING ET AL. IS
IMPROPER

The Examiner rejected dependent Claims 5-9, 13, 18, 23, and 29 over Warren in view of Goffin et al. and Harding et al. These dependent claims are patentable as being dependent upon patentable independent claims, such patentability established in the arguments above.

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**

CONCLUSIONS

In view of the foregoing arguments, it is submitted that all of the claims are patentable over the prior art. Accordingly, the Board of Patent Appeals and Interferences is respectfully requested to reverse the earlier unfavorable decision by the Examiner.

Respectfully submitted,

JACK G. ABID
Reg. No. 58,237
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Appellants

14

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**
_____ /

APPENDIX A - CLAIMS ON APPEAL
FOR U.S. PATENT APPLICATION SERIAL NO. 10/817,148

1.   A semiconductor integrated circuit to execute application code to be received from a memory via external connections, comprising:

a processor to execute the application code from the memory;

an internal bus to provide the application code to the processor from the memory;

a verifier processor to receive the application code via the internal bus, wherein the verifier processor continually processes the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, and to impair the function of the integrated circuit in an event that the application code does not satisfy the verification function; and

an instruction monitor to monitor code requests issued by the processor and to impair the function of the integrated circuit unless addresses of the code requests fall within a given range.

2. The semiconductor integrated circuit according to claim 1 further comprising an internal memory; wherein the given range is stored in the internal memory.

3. The semiconductor integrated circuit according to claim 1 wherein the given range is derived by the verifier processor during a first check of the memory.

4. The semiconductor integrated circuit according to claim 3 wherein the application code in memory comprises a linked list; and wherein the given range comprises a table of linked list addresses.

5. The semiconductor integrated circuit according to claim 3 wherein the verifier processor is to impair the function of the integrated circuit if the verification function is not completed for one complete cycle of the linked list within a predetermined time.

6. The semiconductor integrated circuit according to claim 1 wherein the verifier processor is to receive pause and stop requests and is configured so that any pause and stop request is ineffective during a first check of the code.

7. The semiconductor integrated circuit according to claim 1 wherein the verifier processor is paused for only a predetermined time.

8. The semiconductor integrated circuit according to claim 1 wherein if the application codes does not satisfy the

16

verification function, a reset signal is asserted after a predetermined time.

9. The semiconductor integrated circuit according to claim 8 wherein a status signal is set and stored to indicate that the code does not satisfy the verification function before the reset signal is asserted.

10. The semiconductor integrated circuit according to claim 1 wherein the verification function includes a hash function on the application code.

11. The semiconductor integrated circuit according to claim 1 wherein the verifier processor is to receive a stored secret from the memory; and wherein the verification function comprises a comparison of the secret and the processed application code.

12. The semiconductor integrated circuit according to claim 1 wherein the verification function comprises:
hashing the application code to produce hashed code;
retrieving a signature of the application code from a signature store within the memory; and
verifying the hashed code and the signature using a public key.

13.   The semiconductor integrated circuit according to claim 1 wherein the verifier processor comprises a stop input; and wherein the verifier processor is to restart a given time period after a stop and does not stop again until completing the verification function on the application code at least once.

14.   The semiconductor integrated circuit according to claim 1 wherein the verifier processor is to request portions of the application code from the memory at intervals between requests by the processor for portions of the application code.

15.   The semiconductor integrated circuit according to claim 14 wherein the verifier processor is to request portions of application code at less frequent intervals than the processor.

16.   The semiconductor integrated circuit according to claim 14 wherein the verifier processor is to request portions of the application code at pseudo random times.

17.   The semiconductor integrated circuit according to claim 14 wherein the verifier processor is to carry out read requests at a faster rate during a first check than in subsequent checks.

18.   The semiconductor integrated circuit according to claim 1 wherein impairing the function of the integrated circuit comprises resetting the integrated circuit.

19.   A semiconductor integrated circuit to execute application code to be received from a memory, comprising:

a processor to execute the application code from the memory;

an internal bus connected to the processor to provide the application code to the processor from the memory;

a verifier processor to receive the application code via the internal bus, wherein the verifier processor processes the application code using a verification function while the processor executes the application code from the memory independently of the verifier processor, and to impair the execution of the integrated circuit if the application code does not satisfy the verification function; and

an instruction monitor to be connected to the internal bus, to monitor code requests issued by the processor, and to impair the execution of the integrated circuit unless addresses of the code requests fall within a given range.

21.   The semiconductor integrated circuit of claim 19 wherein the given range is derived by the verifier processor during a check of the memory.

22. The semiconductor integrated circuit of claim 19 wherein the application code in memory comprises a linked list; and wherein the given range is stored in a table of linked list addresses.

23. The semiconductor integrated circuit of claim 19 wherein the verification processor is to impair the execution of the integrated circuit by asserting a reset signal to the processor if the application code does not satisfy the verification function within a predetermined time.

24. The semiconductor integrated circuit of claim 19 wherein the verification processor includes:

an internal processor to coordinate processing of the application code using the verification function and to impair the execution of the integrated circuit if the application code does not satisfy the verification function;

a code memory to be coupled to the internal processor, to store code for controlling the internal processor to process the application code, and to impair the execution of the integrated circuit if the application code does not satisfy the verification function; and

an interface circuit to be connected to the internal processor with the internal bus.

25.   A memory system, comprising:

a non-volatile memory to store application code; and

a semiconductor integrated circuit to execute the
application code to be received from the non-volatile memory,
the integrated circuit including:

a processor to execute the application code
from the non-volatile memory,

an internal bus connected to the processor
to provide the application code to the processor
from the non-volatile memory;

a verifier processor to receive the application
code via the internal bus, wherein the verifier
processor processes the application code using a
verification function while the processor executes the
application code from the non-volatile memory
independently of the verifier processor, and to render
the memory system at least partly unusable if the
application code does not satisfy the verification
function, and

an instruction monitor to be connected to the
internal bus, to monitor code requests issued by the
processor, and to impair the execution of the
integrated circuit unless addresses of the code
requests fall within a given range.

27. The memory system of claim 25 wherein the given range is derived by the verifier processor during a check of the non-volatile memory.

28. The memory system of claim 25 further comprising an internal memory; wherein the non-volatile memory includes a linked list for accessing the application code; and wherein the given range is stored in the internal memory of the integrated circuit as a table of linked list addresses.

29. The memory system of claim 25 wherein the verification processor is to impair the execution of the integrated circuit by asserting a reset signal to the processor if the application code does not satisfy the verification function within a predetermined time.

30. The memory system of claim 25 wherein the verification processor includes:

an internal processor to coordinate the processing of the application code using the verification function and to impair the execution of the integrated circuit if the application code does not satisfy the verification function;

a code memory to be coupled to the internal processor, to store code for controlling the internal processor to process the application code, and to impair the execution of the

integrated circuit if the application code does not satisfy the verification function; and

an interface circuit to be connected to the internal processor with the internal bus.

31. A method for executing application code received from an external memory via external connections, the method comprising:

executing application code from the external memory with a processor;

providing the application code to the processor via an internal bus;

providing the application code to a verifier processor via the internal bus;

continually processing the application code with the verifier processor, while the processor executes the application code independently of the verifier processor, using a verification function;

monitoring code requests issued by the processor with an instruction monitor; and

impairing operation of the integrated circuit if the application code does not satisfy the verification function or if addresses of the code requests fall outside a given range.

32. The method of claim 31 further comprising deriving the given range with the verifier processor during a

check of the external memory.

33.   The method of claim 31 further comprising storing the given range in an internal memory.

34.   The method of claim 31 further comprising:

receiving pause and stop requests at the verifier processor; and

configuring the verifier processor so that any pause and stop request is ineffective during a first check of the code.

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**
_____/

APPENDIX B – EVIDENCE APPENDIX
PURSUANT TO 37 C.F.R. § 41.37(c)(1)(ix)

None.

In Re Patent Application of:
DELLLOW ET AL.
Serial No: **10/817,148**
Filing Date: **APRIL 2, 2002**
_____/

APPENDIX C – RELATED PROCEEDINGS APPENDIX
PURSUANT TO 37 C.F.R. § 41.37(c)(1)(x)

None.